



# Java Secure Socket Extension (JSSE) API

**Brad R. Wetmore**  
Java Security Engineer  
Sun Microsystems, Inc.

# Agenda

- Overview of problem
- High-level JSSE/SSL/TLS overview
- JSSE API
- JSSE Reference Implementation (RI)
  - RI FAQ's
- Export Issues/Futures
- Q&A

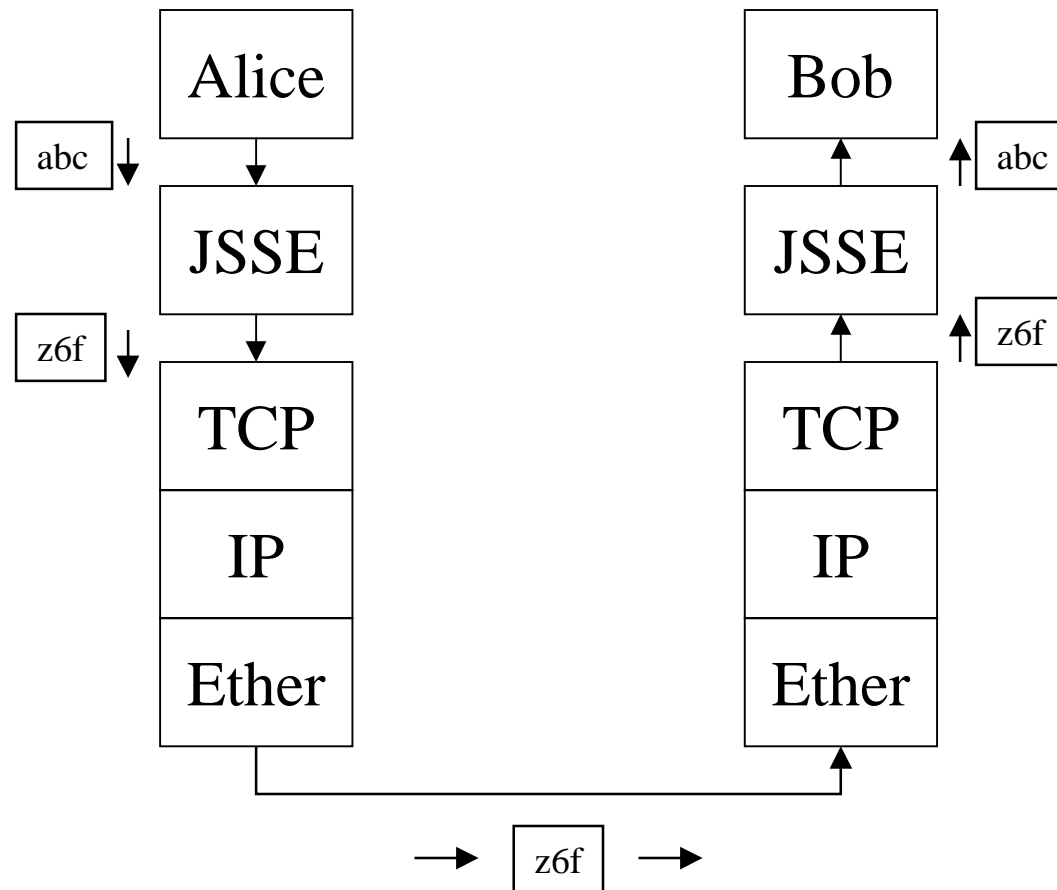


# What Is JSSE?

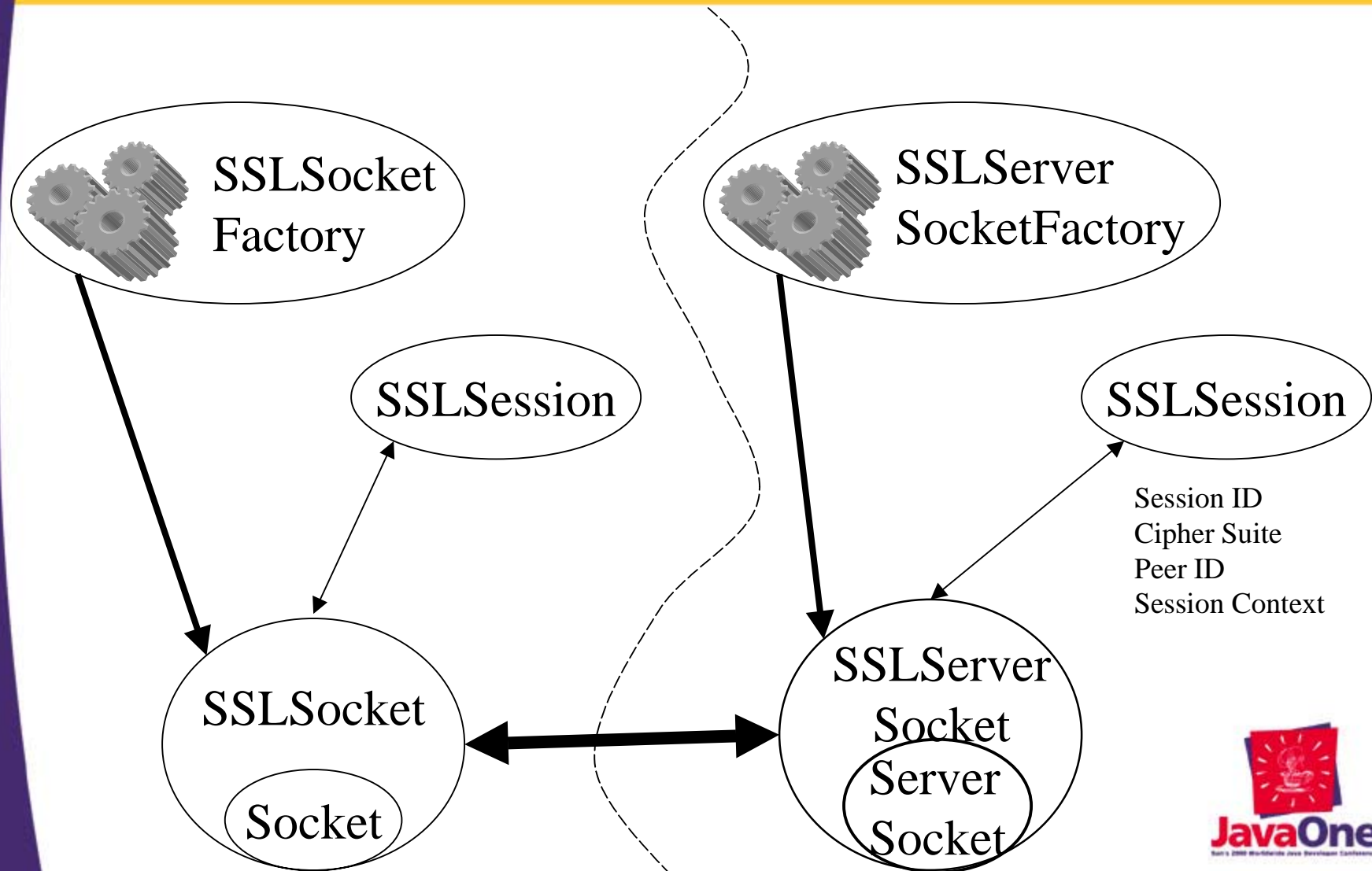
- **Provides for secure networking communications**
  - Data encryption
  - Authentication
  - Message integrity
- **<http://java.sun.com/products/jsse>**
  - API
  - RI, Ver. 1.0.1, March 2000
    - Distribution:
      - domestic, global, docs-only, sample code



# Where JSSE fits into TCP/IP



# API Overview



# JSSE Client Code Example

```
/*
 * Use SSL, a non-SSL socket would use:
 *     Socket socket = new Socket (www.sun.com, 80);
 */
SSLSocketFactory factory = (SSLSocketFactory) SSLSocketI
SSLSocket socket = (SSLSocket) factory.createSocket(
    "www.sun.com", 443);

PrintWriter out = new PrintWriter(
    new BufferedWriter(
    new OutputStreamWriter(
    socket.getOutputStream())));

out.println("GET http://www.sun.com/index.html HTTP/1.1")
out.flush();
```



# Other JSSE (javax) Entities

- **SSLSessionContext**
  - Group of SSLSessions available for an entity
- **SSLBindingEvent**
  - notification of objects bound to SSL Session
- **HandshakeCompletedEvent**
- **Duplication of Certificate Classes**
  - Code was written before Java SDK 2
  - Most are wrapper classes to Java 2 certs.



# Sun's RI Details

- **100% Java**
- **Requires JDK 1.2.1**
- **Free for commercial deployment**
  - Check licensing for details
- **Supports SSL v3.0, TLS v1.0**
- **Various algorithms built-in**
  - RSA, RC4, DES, 3DES, DH, DSA, SHA, MD5
  - Apps. can not access algs. directly (JCA)
- **https support**





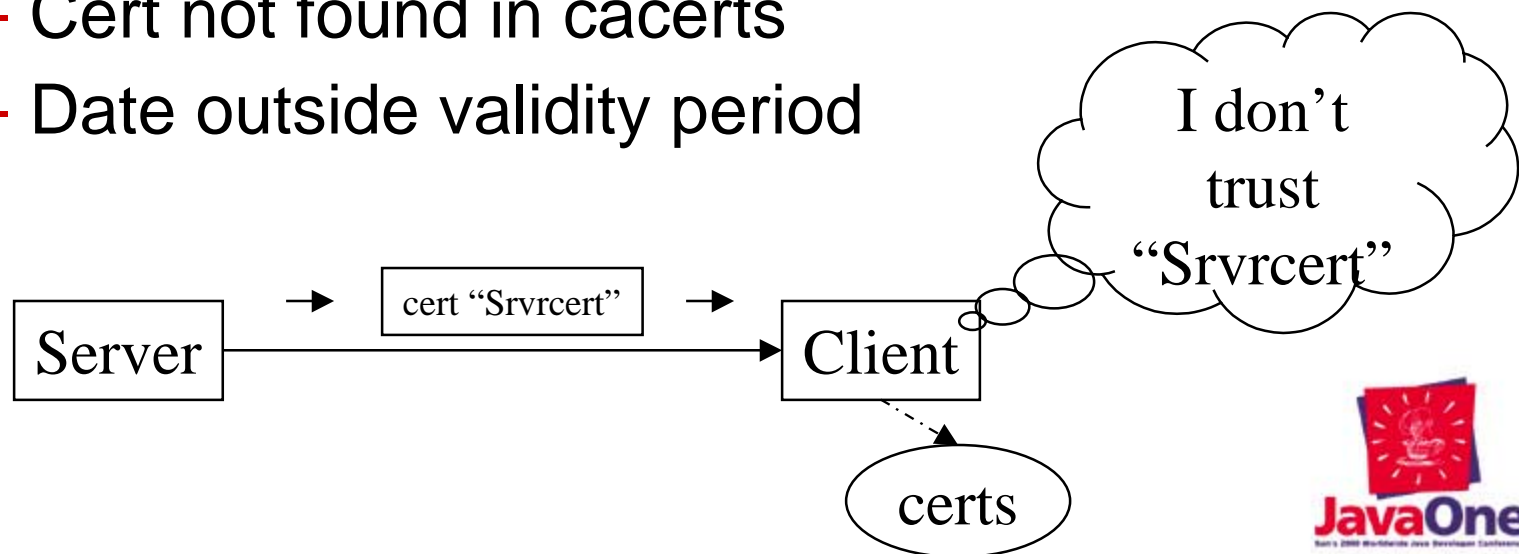
# Sun's RI Details (#2)

- **com.sun.net.ssl**
  - Internal package, subject to change
  - SSLContext
    - Secure socket protocol information
    - Source of SSLSocketFactories
  - KeyManager
    - Source of key material
  - TrustManager
    - Makes trust decisions
  - All use the JCA “SPI” mechanism
    - Can replace SSLContext, KeyManager, TrustManager



# FAQ's

- **Java-security@sun.com archives**
- **Installation problems**
- **Visual Cafe's certificate file**
- **“untrusted \_\_\_\_\_ cert chain”**
  - Cert not found in cacerts
  - Date outside validity period



# Export Issues/Futures

- **“Hasn’t the US relaxed export restrictions? How come JSSE...”**
  - Not an easy or quick process
  - Minor mods to RI needed
- **JSSE 1.0.2**
  - Support for strong global crypto.
  - Will also support PJava 3.1
- **Move JSSE RI into Merlin**



# Feedback & Support

- **For feedback on the JSSE API**
  - java-security@sun.com
- **For business questions**
  - java-security-business@sun.com
- **For support with the JSSE RI**
  - <http://www.sun.com/developer/support/>



# Various URLs

**<http://java.sun.com/products/jsse>**

<http://archives.java.sun.com/archives/java-security.html>

[http://www.epic.org/crypto/export\\_controls](http://www.epic.org/crypto/export_controls)

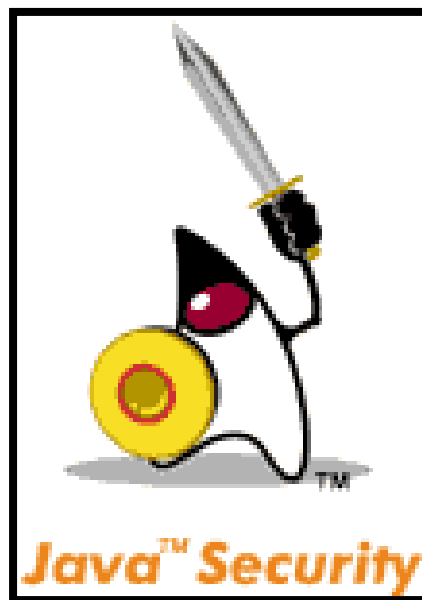
<http://developer.netscape.com/docs/manuals/security.html>

<http://home.netscape.com/eng/ssl3/ssl-toc.html>

<http://www.ietf.org/rfc/rfc2246.txt>



# Q & A





**JavaOne**<sup>SM</sup>  
Sun's 2000 Worldwide Java Developer Conference™